INFORMATION OPERATIONS
&
SECURITY

Date: 6 MAR 2013

DR. ROBERT HERKLOTZ
PROGRAM OFFICER
AFOSR/RTC
Air Force Research Laboratory

Integrity ★ Service ★ Excellence

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
06 MAR 2013		**00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Operations and Security	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Office of Scientific Research ,AFOSR/RTC,875 N. Randolph,Arlington,VA,22203**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the AFOSR Spring Review 2013, 4-8 March, Arlington, VA.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**34**	

2013 AFOSR SPRING REVIEW

NAME: DR. ROBERT HERKLOTZ

BRIEF DESCRIPTION OF PORTFOLIO:

Fund science that will enable the AF and DOD to dominate cyberspace: Science to develop secure information systems for our warfighters and to deny the enemy such systems.

LIST SUB-AREAS IN PORTFOLIO:

1: SOS-Science of Security
2: Secure Humans
3: Secure Networks
4: Secure Hardware
5: Covert Channels
6: Execute on Insecure Systems
7: Secure Data
8: Secure Systems-Security Policy

PROGRAM STRATEGY

- **FEEDBACK FROM LAST YEAR: GOOD RESEARCH BUT PROGRAM LACKING STRATEGY**

- **THIS YEAR: WILL FOCUS ON PROGRAM STRATEGY**

INFO OPS AND SECURITY STRATEGY

- FOLLOW NATIONAL, DOD, AF, AFRL AND AFOSR STRATEGIES
- ANTICIPATE FUTURE ATTACKS: OFFENSIVE AND DEFENSIVE ASPECTS OF CYBER SECURITY THE SAME AT BASIC RESEARCH LEVEL
- TEAM AND LEVERAGE OTHER AGENCY INVESTMENTS: DOD, NSA, NIST, ARO, ONR, NSF, DARPA, IARPA, DOE
- FIND NICHE FOR LIMITED BUDGET

CYBER SECURITY BACKGROUND: PROBLEM

- UNENDING ATTACK-PATCH-ATTACK CYCLE
- INVESTMENT BARELY KEEPS UP WITH NEW ATTACKS AND IS AFTER THE FACT-RESOURCE CONSTRAINTS
- ASSYMENTRIC ADVANTAGE FOR ATTACKER
  - GROWING CYBERSPACE THREATS AND VULNERABILITIES
  - INCREASED DEPENDENCY ON CYBER
  - CAN CHOOSE TIME AND LOCATION
  - MUST DEFEND WHOLE OF NETWORKED SYSTEMS
  - MORE AGILE
  - NO RULES
  - JUST AS SMART AS DEFENDERS

CYBER SECURITY BACKGROUND: FIX

- AFTER MANY STUDIES A NEW NATIONAL STRATEGY
  - RAISE THE BAR FOR THE ATTACKER
  - DISCOVER HOW TO BUILD INHERENTLY SECURE SYSTEMS

- RAISE THE BAR
  - INCREASE WORKLOAD TO EXECUTE ATTACK
  - INCREASE TIME TO PLAN ATTACK

- INHERENTLY SECURE: SCIENCE OF CYBER SECURITY
  - SYSTEM: SOFTWARE, HARDWARE, NETWORK, HUMANS
  - FORMALLY DEFINE CYBER SECURITY: DISCOVER AND DEFINE BASIC SYSTEM PROPERTIES THAT COMPOSE SYSTEM SECURITY
  - DEVELOP SCIENTIFIC FOUNDATIONS

RAISE THE BAR

- DOD STUDY (PRIORITY STEERING COUNCIL STUDY)
  - ASSURING EFFECTIVE MISSIONS
  - AGILITY
  - RESILIENCY
- AF-CYBER VISION 2025 STUDY
  - MISSION ASSURANCE AND EMPOWERMENT
  - AGILITY AND RESILIENCY
  - OPTIMIZED HUMAN-MACHINE SYSTEMS
- FOUNDATIONAL SCIENCE 4TH BULLET IN BOTH STUDIES

QDR Cyber S&T Study
Top Enabling Technologies

Tier 1:

- *Distributed Trust*
- *Resilient Architectures*
- *Response and Cyber Maneuver*
- *Visualization and Decision Support*

Tier 2:

- Component Trust
- Detection and Autonomic Response
- Recovery and Reconstitution

Tier 3:

- Advanced Cross-Domain Solutions
- Advanced Cryptography
- Quantum Computing, Comms, and Crypto
- Biometrics
- Code Verification and Compliance
- Correct (Assured) by Construction Software
- Deception and Information Hiding
- Human Factors and Training
- Malware/Forensics Analysis and Reverse Engineering
- Resilient Infrastructure and Comms
- Scientific Theory and Measures
- Sensing and Data Fusion
- Software Pedigree and Provenance

Cyber PSC Research Roadmap

Desired End State

Resiliency	Agility	Assuring Effective Missions
• Missions are difficult to disrupt even when attacks on cyber infrastructure are successful • Hardware, software, and applications have built-in features and architectural provisions to withstand damage and will still operate to carry out their functions	• Systems and services at all levels of the cyber infrastructure have the ability to provide rapid-risk-driven control, adaptation, and maneuver of their configurations, interactions, and mechanisms • Threats are reduced or countered by confounding adversary attacks and assumptions	• Commanders seamlessly orchestrate the cyber element of both kinetic and non-kinetic operations • Commanders maintain full understanding and control of the situation in real time, while denying adversaries the same • Missions are conducted with well-informed consideration of options and tradeoffs for achieving desired effects, and with a comprehensive view of how mission outcomes depend on the cyber components

Cross-Cutting: Foundations of Trust

- Cyber elements are employed with a quantitative and known level of confidence (empirically or theoretically based) that their identity, functionality, and content are as expected
- High confidence components can be created from mixed confidence elements
- Measurable and predictable levels of trust enable a quantitative approach to design, tradeoff analysis, and risk mitigation

Air Force Cyber Vision 2025 Findings

- **Mission at risk: Interdependency growth driving cost and risk; Insider threat, supply chain threat, Advanced Persistent Threat (APT)**
- **Cyber S&T enables: assurance, resilience, affordability, empowerment**
- **Need to integrate across authorities and domains**

DEVELOP SCIENTIFIC FOUNDATIONS

Developing Scientific Foundations – Developing an organized, cohesive scientific foundation to the body of knowledge that informs the field of cybersecurity through adoption of a systematic, rigorous, and disciplined scientific approach. **Promotes the discovery of laws, hypothesis testing, repeatable experimental designs, standardized data-gathering methods, metrics, common terminology, and critical analysis that engenders reproducible results and rationally based conclusions.**

CV25 S&T Themes (1/2)

- Mission assurance and empowerment
  - Survivability and freedom of action in contested and denied environments
  - Enhanced cyber situational awareness for air, space, and cyber commanders enabled by automated network and mission mapping
  - Ability to detect and operate through cyber attacks enabled by threat warning, integrated Intelligence (e.g., SIGINT, HUMINT, IMINT), and real-time forensics/attribution
  - Early vulnerability detection and enemy behavior forecasting enabled by advanced cyber ranges, including high fidelity, real-time modeling and simulation
  - Cross domain integrated effects and cross domain measures of effectiveness (MOEs), including cyber battle damage assessment

- Agility and resiliency
  - Effective mix of redundancy, diversity, and fractionation for survivability
  - Reduction of attack surface, critical mission segregation, and attack containment
  - Autonomous compromise detection and repair (self healing) and real-time response to threats
  - Transition from signature based cyber sensors to behavior understanding to enhance high performance attack detection
  - Active defense requires rapid maneuver enabled by dynamic, reconfigurable architectures (e.g., IP hoping, multilevel polymorphism)

CV25 S&T Themes (2/2)

- **Optimized human-machine systems**
  - **Measurement of physiological, perceptual, and cognitive states to enable personnel selection, customized training, and (user, mission, and environment) tailored augmented cognition.**
  - **High performance visualization and analytic tools to enhance situational awareness, accelerate threat discovery, and empower task performance.**
  - **Autonomy appropriately distributed between operators and machines, enabled by increased transparency of autonomy and increased human "on the loop" or supervisory control.**

- **Software and hardware foundations of trust**
  - **Operator trust in systems (e.g., sensors, communications, navigation, C2) enabled by trusted foundries, anti-tamper technologies, and supply chain assurance, as well as effective mixes of government, commercial off the shelf, and open source software**
  - **Formal verification and validation of complex, large scale interdependent systems**
  - **Advanced vulnerability analysis, automated reverse engineering, real-time forensics tools**
  - **High speed encryption, quantum communication, and quantum encryption for confidentiality and integrity**

INFO OPS AND SECURITY NICHE

- DEVELOP SCIENCE OF CYBER SECURITY
- DEVELOP METHODS TO EXECUTE MISSION SECURELY ON INSECURE SYSTEMS
- INVENT THEORY AND METHODS TO DISCOVER COVERT CHANNELS, SIDE CHANNELS, HIDDEN SOFTWARE, HIDDEN CIRCUITS IN HARDWARE

A Science Of Security?

A **body of laws** that are predictive…

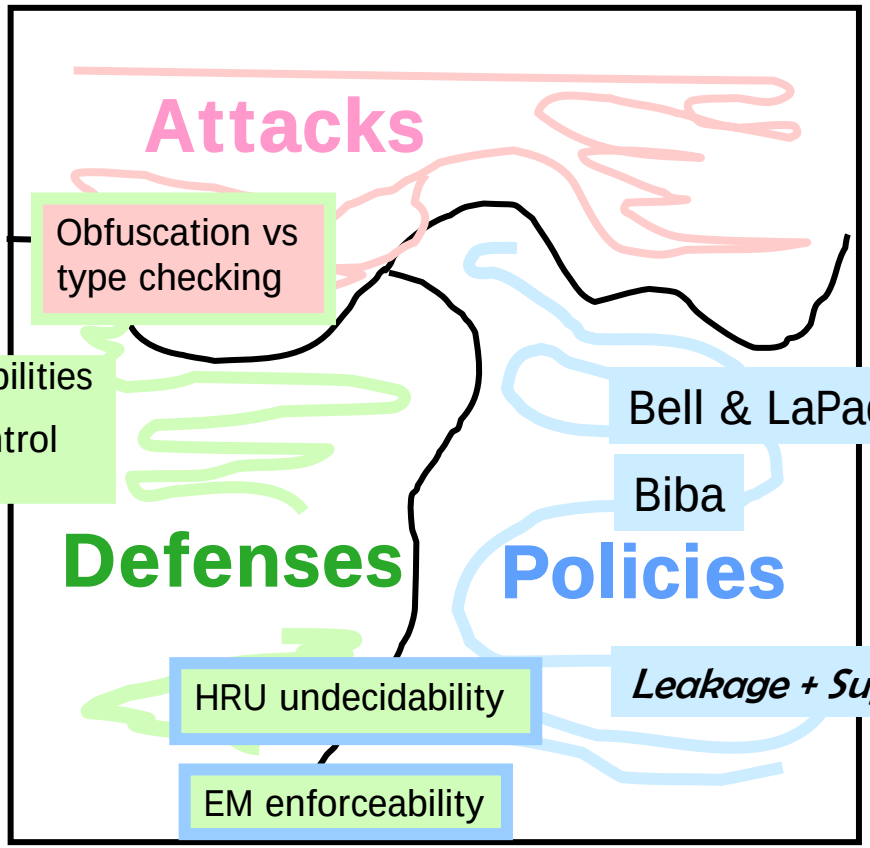
- Transcend specific systems, attacks, and defenses.
- Applicable in real settings.
- Provide explanatory value.
  - Abstractions and models
  - Connections and relationships. E.g.,
    - Cannot enforce policy P with mechanism M
    - Interface can leak b bits/sec

Kinds of Laws

- **Analysis**: **Given an artifact, predict its properties…**
  - Qualitative properties: What it does.
  - Quantitative properties: How well it works.

- **Synthesis: Compose artifacts with given properties to obtain a new one with predictable properties.**

Laws About What?



Classes of policies
Classes of attacks
Classes of defenses

Relationships:
"Defense class D enforces policy class P despite attacks from class A."
"Defense D + Defense D' = …"

HONORS AND TRANSITIONS

ACM Special Interest Group on Security, Audit and Control (SIGSAC)

SIGSAC Outstanding Contribution Award: This award is given for significant contribution to the field of computer and communication security through fostering research and development activities, educating students, or providing professional services such as the running of professional societies and conferences.

2012 SIGSAC Outstanding Contribution Award: **Robert Herklotz**, U.S. Air Force Office of Scientific Research, for contributions to Air Force information systems security. His efforts provided the science foundation to enable development of advanced cyber security methods, models, and algorithms to support future Air Force systems.

HONORS AND TRANSITIONS

Latifur Khan, UTD: Technical Achievement Award presented jointly by the IEEE Systems, Man and Cybernetics Society and IEEE Transportation Systems Society.

Joe Halpern, Cornell: awarded the Ray Reiter Best Paper award at KR 2012 (Conference on Principles of Knowledge Representation and Reasoning).

Kevin Hamlen and Zhiqiang Lin, UTD: best paper award at the ACSAC, also got the AT&T second prize among all the applied cyber security research papers published in 2012.

Eunice Santos, UTEP: Elected to Fellow for AAAS

Judea Pearl, UCLA: ACM A.M. Turing Award for Contributions to AI

Eugene Santos Jr, Dartmouth: Elected Fellow by IEEE

HONORS AND TRANSITIONS

R. R. Brooks, Clemson:
Detect use of tunneled communications protocols and infer their current internal state

- Private communications often tunneled through virtual private networks (VPNs)
- Mix networks tunnel connections for anonymity
- Tunneling tools (ex. ssh, ssl, TOR) have timing vulnerabilities
- Hidden Markov models (HMM) and probabilistic grammars to detect protocol use, infer network flows, partially decipher content

Transitions:

- Technology results used in operational classified programs and integrated into US Navy and NATO operations
- Dept of State Internet Freedom project for West Africa
- AFRL SBIR with Sentar Inc.
- BMW Manufacturing Corp DLP

HONORS AND TRANSITIONS

Keesook Han, AFRL/RIGA: started two CRADAs with MITRE
1. AFRL/MITRE CRADA: AFOSR in-house Botnet Research
2. AFRL/MITRE CRADA: AFOSR in-house Cloud Auditing and Android Smartphone Security

Nadia Heninger, UCSD: A flaw has been found in the encryption system used to conceal from cybercriminals data passed between parties in online shopping, banking, e-mail and other Internet services. The flaw is in the way the public-key cryptography system generates random numbers to prevent others from deciphering digital messages.
The flawed keys mainly affected various types of embedded devices, such as routers and virtual private networks, not "full-blown Web servers." "There's no need to panic," she said. However, Heninger said she and several colleagues in a separate study were able to **remotely compromise about 0.4 percent of all the public keys used in SSL Web site security**. SSL, or Secure Sockets Layer, is the cryptographic protocol for securing communications over the Internet. "We've found vulnerable devices from nearly every major manufacturer," Heninger said. The team plans to release their report after contacting all the manufacturers with products that may be affected.

Cyber Trust and Suspicion

Eunice E. Santos
Institute of Defense & Security
University of Texas
El Paso, TX
eesantos@utep.edu

Eunice E. Santos

Objectives

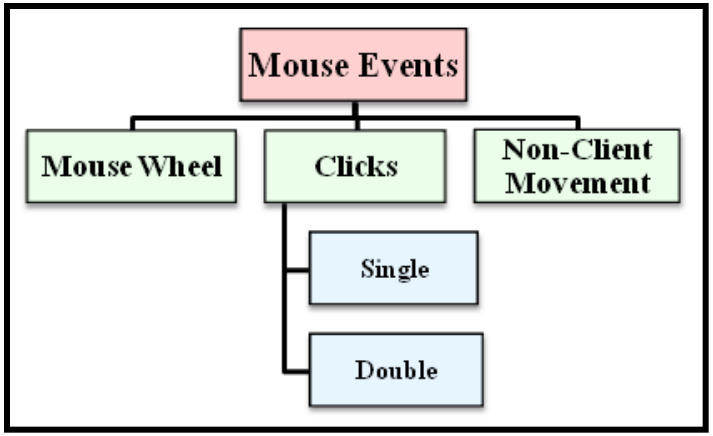
- Developing a model of insider behavior that accounts for and explains the social, cultural, and emotional basis for trust and suspicion especially its impacts on insider threat.
- Research and identify biomarkers of cyber trust for the selection of targeted training and interface/alert interventions.
- Systematically demonstrate and examine how human performance affects cyber security operations with humans in the loop, and explore how such effects can be mitigated or exploited in order to achieve a higher-level of security.
- Conduct human subject studies (where subjects are equipped with non-invasive sensors) to provide real-time predictions about the changing level of trust and suspicion experienced by subjects while they conduct tasks that are designed specifically to test hypotheses stemming from the other team members' research.
- Assess, attribute, and manipulate operator suspicion through cyber means and demonstrating formal models of suspicion.

Suspicion Detection-Keystroke Dynamics

- Correlation has been found between keystroke timings and changes to mental state, such as cognitive workload and deception under the Deny and Disrupt (DnD) effort
  - Traditional Timing Features
    - Key Hold Time (KHT) – Keystroke duration (aka dwell time)
    - Key Interval Time (KIT) – Time between the release of one key and the press of another (aka flight time)
    - Key Press Latency (KPL)
    - Key Release Latency (KRL)
  - User Features
    - Frequency of errors
    - Use of numpad
    - Use of shift keys (order and which shift key)
    - Use of shortcut keys

Suspicion Detection-Mouse Dynamics

- Investigate features from past mouse dynamics research for applicability to mental state
  - Pusara & Brodley (2004) calculated: distance, angle, and speed for selected pairs of points within temporal windows of data.
  - Schulz (2006) examined features of curves within mouse movement (e.g. curve length, number of points within curvature area, and inflection points) and computed a histogram of typical mouse movement curves for each user.
  - Ahmed & Traore (2007) used mouse movement, drag & drop, point & click, and silence (non-movement) for a histogram.
    - Calculated traveled distance, action type, movement direction, average movement speed, movement speed versus travelled distance, and time elapsed during movement
  - Feher, et al. (2012) created hierarchy from individual mouse movements to elaborate sequences and calculated “trajectory center of mass” and “third and fourth” moment.



Pusara & Brodley (2004) classify mouse data into a hierarchy of mouse events. Non-client movement refers to movement within an applications title and menu bars.

Suspicion Detection-Other Cyber Sensors

- **Investigate other potential Cyber Sensors**
  - User Preferences Sensor
    - Application usage profile
    - Usage time
    - Login times
    - Perform anomaly detection
  - System Call Monitors
    - Monitor system calls/other low-level system APIs
    - Monitor registry access
    - Determine users behavior in response to a change in mental state or the occurrence of a D5 effect
    - Profile user: level of knowledge, technical sophistication, etc.
  - Application-specific Sensors
    - Determine which buttons are pressed in a GUI
    - Identify specific menu options utilized
    - Popular and technically informative applications
      - Windows Task Manager
      - Microsoft Word

Towards a Science Base for Cybersecurity

Fred B. Schneider
fbs@cs.cornell.edu
CS Department
Cornell University

AFRL

VALUE OF INFORMATION

Thesis: A science base for cybersecurity must include a expressive account of information flow.

- **Approaches to quantifying the value of information that flows.**
- **Means for specifying and enforcing re-classification of information.**

Adding Value to Information

Classical view of information [Shannon]

- **Unit of information: bit**
- **All bits have equal value.**
  - **Over-simplification:**
    - High-order vs low-order digits of a salary.
    - Alternative representations for a location:
      - Lat / Lon coordinates -versus-
      - House number, street name, city name, country

Scaling Defenses to Protect Value

Classical view of defense:

- Assign a value to each asset.
- Choose defenses based on those values:
  - Cost of circumventing a defense should be proportional to value of asset being protected.

… Requires knowing the value of the information that some defense allows to leak or be corrupted?

A Valued Information Theory

(Joint work with Mario Alvim and Andre Scedrov, Univ of Penn)

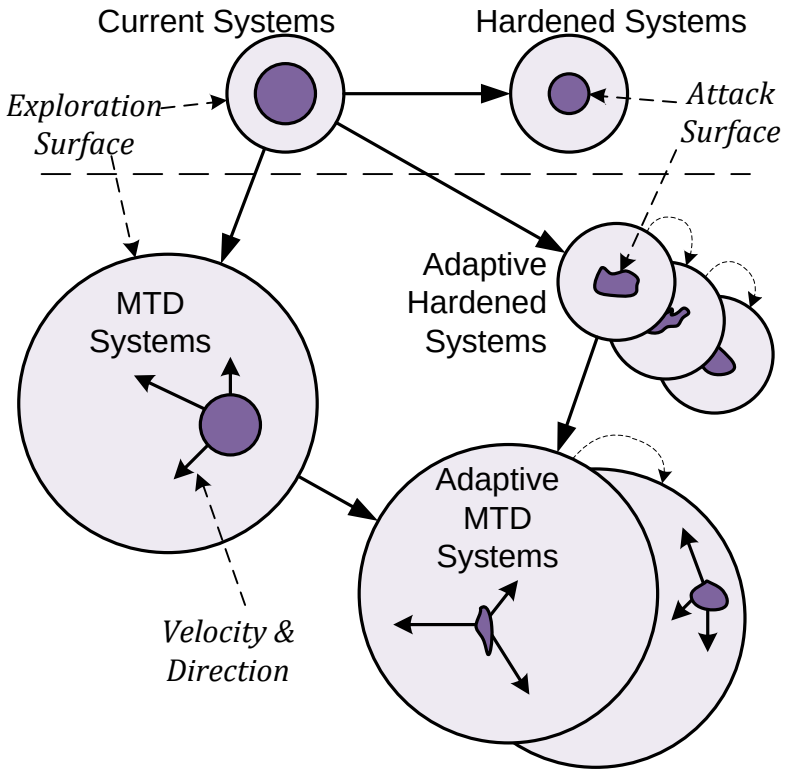
- **Extended Shannon's information theory to assign values to information (rather than to bits).**
- **Developed measures analogous to entropy for information that is leaked / transmitted / corrupted / suppressed by attacks:**
  - **expected value learned in a single attack,**
  - **probability of learning specified value in single attack,**
  - **expected number of attack steps to learn a specified value.**
- **Proved "reasonableness" properties for measures.**

Understanding and Quantifying the Impact of Moving Target Defenses on Computer Networks

Scott A. DeLoach and Xinming Ou
Computing & Information Sciences
Kansas State University
October 3, 2012

AFRL

High-level Intuition of MT Network Defense



- **Current approaches shrink and harden attack surface**
- **MTDs move attack surface *and* expand exploration surface**
- **Adaptive MTDs move and modify attack surface**

Our Research Objectives

- **Understand and quantify the potential and limitations of MTDs for computer networks**
- **Our approach**
  - **Develop analytical models to quantify MTD effectiveness**
  - **Conduct scientific experimentation to examine the cost/benefit of MTD on computer networks**
  - **Design a proof-of-concept MTD system to demonstrate concepts and validate models**